SEGURIDAD INFORMÁTICA

Resultados de aprendizaje y criterios de evaluación:

1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades

Criterios de evaluación:

a) Se ha valorado la importancia de mantener la información segura.
b) Se han descrito las diferencias entre seguridad física y lógica.
c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.
d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.
e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.
f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.
g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.
h) Se ha valorado la importancia de establecer una política de contraseñas
i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.

2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.

Criterios de evaluación:

a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.
b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).
c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.
d) Se han descrito las tecnologías de almacenamiento redundante y distribuido. e) Se han seleccionado estrategias para la realización de copias de seguridad.
f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.
g) Se han realizado copias de seguridad con distintas estrategias.
h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.
i) Se han utilizado medios de almacenamiento remotos y extraíbles.
j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.

SEGURIDAD INFORMÁTICA

3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.

Criterios de evaluación:

a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.
b) Se han clasificado los principales tipos de software malicioso.
c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.
d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.
e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.
f) Se han aplicado técnicas de recuperación de datos.

4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.

Criterios de evaluación:

a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.
b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.
c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.
d) Se han aplicado medidas para evitar la monitorización de redes cableadas.
e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.
f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.
g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.
h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.

5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.

Criterios de evaluación:

a) Se ha descrito la legislación sobre protección de datos de carácter personal.
b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.
e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
f) Se han contrastado las normas sobre gestión de seguridad de la información.

SEGURIDAD INFORMÁTICA

6. Cumple las normas de prevención de riesgos laborales y de protección ambiental, identificando los riesgos asociados, las medidas y equipos para prevenirlos.

Criterios de evaluación:

a) Se han identificado los riesgos y el nivel de peligrosidad que suponen la manipulación de los materiales, herramientas, útiles, máquinas y medios de transporte.
b) Se han operado las máquinas respetando las normas de seguridad.
c) Se han identificado las causas más frecuentes de accidentes en la manipulación de materiales, herramientas, máquinas de corte y conformado, entre otras.
d) Se han descrito los elementos de seguridad (protecciones, alarmas, pasos de emergencia, entre otros) de las máquinas y los equipos de protección individual (calzado, protección ocular, indumentaria, entre otros) que se deben emplear en las operaciones de montaje y mantenimiento.
e) Se ha relacionado la manipulación de materiales, herramientas y máquinas con las medidas de seguridad y protección personal requeridos.
f) Se han identificado las posibles fuentes de contaminación del entorno ambiental.
g) Se han clasificado los residuos generados para su retirada selectiva.
h) Se ha valorado el orden y la limpieza de instalaciones y equipos como primer factor de prevención de riesgos.

Contenidos mínimos:

Instalación de software libre y propietario:

- Ubicación y protección física de los equipos y servidores.
- Sistemas de alimentación ininterrumpida.
- Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad.
- Almacenamiento redundante y distribuido.
- Almacenamiento remoto y extraíble.
- Cifrado y Criptografía de datos.
- Copias de seguridad e imágenes de respaldo.
- Medios de almacenamiento.
- Implementación de listas de control de acceso.
- Identificación digital. Firma electrónica y certificado digital. Implementación.
- Seguridad en los protocolos para comunicaciones inalámbricas.
- Tunneling seguro. IPSec. VPN's. SSH. Implementación y utilización de cortafuegos en un sistema o servidor.
- Política de contraseñas.
- Recuperación de datos desde copias de seguridad. Software malicioso. Clasificación. Herramientas de protección y desinfección.
- Métodos para asegurar la privacidad de la información transmitida.
- Fraudes informáticos y robos de información. Estudio de casos
- Control de la monitorización en redes cableadas.
- Seguridad en redes inalámbricas peculiaridades e implementaciones.
- Sistemas de identificación: firma electrónica, certificados digitales y otros.
- Cortafuegos: funcionalidad básica en equipos y servidores dedicados.
- Zonas desmilitarizadas (redes perimetrales)

SEGURIDAD INFORMÁTICA

- Legislación sobre protección de datos.
- Legislación sobre los servicios de la sociedad de la información y correo electrónico.